

Status	of 26.12.2008 - has terminated
(11) Number of the patent document	2091983
(13) Kind of document	C1
(14) Document date	1997.09.27
(19) Publishing country or organization	RU
(21) Application number registered	93007865/09
(22) Application filing date	1993.02.09
(45) Date	1997.09.27
(516) Edition of IPC	6
(51) Main classification IPC	H04L9/00
(51) Main classification IPC	G06F12/16
Title	METHOD OF CODING OF BINARY INFORMATION AND DEVICE FOR ITS REALIZATION
(71) Applicant information	Chizhukhin Gennadij Nikolaevich
(72) Inventor information	Chizhukhin Gennadij Nikolaevich
(73) Grantee (asignee) information	Chizhukhin Gennadij Nikolaevich

#2091983. Abstract

FIELD: cryptography at arrangement of devices of commercial closed communication.

SUBSTANCE: an N-bit secret key is formed, with the aid of which a flow code is formed, summation being modulo 2 with an information text; the flow code is formed as K groups with N bits in each, where $k \leq N$ - length of the text being processed. The first group of the flow code is formed by raising the N-bit secret key to the n power to modulo P, and the second group of the flow code is formed by raising the N-bit code of the first group of the flow code to the n power to modulo P, where n - number of least-significant bits of the secret key with $1 \leq n \leq N \leq P-1$, and each subsequent i group of the flow code, where $i=3,4,\dots,k$, is formed by raising the n-bit code of the i-1 group of the flow code to the m power to modulo P, where m - number of least-significant bits of the i-2 group of the flow code, $m=n$; prior to taking a sum to modulo 2, in each group of the K groups of the formed flow code the bits are mixed in an accidental manner and memorized. The device for realization of the method uses unit 1 for raising to n power to modulo P, power register 2, secret key register 3, key group register 4, sequence bit mixing unit 5, first and second modulo 2 adders 6 and 7, key 8, control unit 9, serial- alternate registers 10₁-10₄, OR gate 11 and AND gates 12 12₁-12₃. EFFECT: enhanced safety of information in computer commercial communication systems. 2 cl, 1 dwg